chrome enterprise

Zero-Trust-Sicherheit mit Chrome Enterprise und BeyondCorp Enterprise

Einführung

Netzwerkfirewalls haben über Jahrzehnte hinweg für Perimetersicherheit bei Unternehmen gesorgt. Wie neueste Datenpannen bewiesen haben, können Angreifer heutzutage jedoch auch die stärksten Firewalls durchbrechen und sowohl dem Betrieb als auch dem Ruf des betroffenen Unternehmens schaden.

In letzter Zeit sind Firewalls sogar noch problematischer geworden, da Unternehmen und ihre Mitarbeiter mehr mobile Geräte und cloudfähige Technologien verwenden.

Die Zero-Trust-Lösung von Google, BeyondCorp Enterprise, sorgt dafür, dass die Zugriffssteuerung nicht mehr über das Netzwerk, sondern auf Nutzerebene stattfindet. Der Zugriff auf Unternehmensressourcen unterliegt Kontextfaktoren in Bezug auf das Gerät und die Anmeldedaten des Nutzers und ist deshalb besser geschützt. Dabei spielt keine Rolle, ob der Nutzer sich tatsächlich in einem Unternehmensgebäude befindet oder von zu Hause aus arbeitet. Solange sein Gerät und seine Anmeldedaten nicht authentifiziert wurden, hat er keinen privilegierten Zugriff auf Netzwerkressourcen.

Mit BeyondCorp Enterprise können IT-Experten den Zugriff auf Unternehmensanwendungen und -ressourcen detailliert steuern. Außerdem wird den Nutzern ermöglicht, von jedem Netzwerk aus zu arbeiten, ohne sich über ein traditionelles VPN mit dem privilegierten Netzwerk verbinden zu müssen.

Google Chrome ist die wichtigste Schnittstelle für Nutzer, die auf sensible geschäftliche Ressourcen zugreifen müssen – ihre sichere Standleitung zum Unternehmen. Die browserbasierten Funktionen von Chrome zur Abwehr von Bedrohungen und die Datenschutzmaßnahmen von BeyondCrop Enterprise bieten Schutz vor Datenverlust in Echtzeit sowie Malware-Scans und URL-Prüfungen – allesamt übersichtlich dargestellt in der Admin-Konsole.

chrome enterprise

Anwendungsfälle

Mit Chrome Enterprise und BeyondCorp Enterprise stehen Ihnen Zero-Trust-Schutzmaßnahmen auf Grundlage erstklassiger Sicherheitstechnologien von Google zur Verfügung – darunter kontextsensitiver Zero-Trust-Zugriff, Datenschutzmaßnahmen und Schutz vor Malware, Phishing und Ransomware (Erpressungstrojaner).

Die Zero-Trust-Funktionen von BeyondCorp Enterprises sorgen in einer Vielzahl von Fällen für die Sicherheit, die ein Unternehmen benötigt. Einige Beispiele:

- Neu eingestellten Mitarbeitern oder Partnern kann ein sicherer Zugriff auf geschäftliche Anwendungen ermöglicht werden, ohne dass dafür ein VPN oder ein lokaler Agent benötigt wird.
- Tabellen mit sensiblen Daten werden nur dann für andere freigegeben, wenn die von Ihnen festgelegten Richtlinien erfüllt sind – beispielsweise beim Zugriff über eine Unternehmens-E-Mail-Adresse oder von einem Gerät aus, das über angemessenen Schutz vor Phishing oder Ransomware verfügt.
- Es lassen sich alle Mitarbeiter identifizieren, die ihre geschäftlichen Passwörter auf externen Websites verwenden. Sie werden automatisch aufgefordert, diese Passwörter zu ändern.
- Mit der Bestätigung in zwei Schritten können Sie privilegierte Ressourcen besser vor schädlichen Angriffen schützen.
- Auf Grundlage von Authentifizierungs- und Kontextinformationen über den Partner und seine Geräte können Sie einen eigens für ihn angelegten Zugriff auf privilegierte Netzwerkressourcen bereitstellen.
- Mit den Datenleck-Schutzfunktionen in ChromeOS und Chrome lässt sich vermeiden, dass Informationen wie geschützte Gesundheitsdaten nach außen gelangen.
- Malware-Übertragungen und laterale Ausbreitung über genehmigte Anwendungen werden verhindert.
- Nutzer werden davon abgehalten, Phishing-URLs aufzurufen, die in E-Mails oder in Anwendungen eingebettet sind.

All diese Funktionen bieten authentifizierten Nutzern eine Ende-zu-Ende-Sicherheit für den Zugriff auf privilegierte Ressourcen, ohne sich spürbar auf die Leistung auszuwirken.

Die Rolle von Chrome in BeyondCorp Enterprise

Der Chrome-Browser erweitert den Wirkungsumfang der Zero-Trust-Sicherheit bis ins Web. Technologien wie Safe Browsing, Website-Isolierung und Sandbox-Funktionen machen Chrome zu einem sicheren Browser für jedes Unternehmen. Seine schnellen und automatischen Updates sorgen dafür, dass Nutzer immer die aktuell sicherste Version verwenden. Mit BeyondCorp Enterprise profitieren Unternehmen sogar von noch mehr Chrome-Schutzfunktionen gegen externe Bedrohungen durch Angreifer, Fehler unvorsichtiger Nutzer, interne Datenpannen und Exfiltrationen.

Da Nutzer die meiste Zeit ihres Arbeitstages mit Aufgaben im Webbrowser verbringen, sollte Chrome als wesentlicher Teil des Zero-Trust-Sicherheitsmodells einer Organisation gelten (Abbildung 1).

chrome enterprise

Mit der browserbasierten Erkennung von Bedrohungen und den Datenschutzfunktionen von Chrome als Teil der Zero-Trust-Strategie Ihres Unternehmens können Sie folgende Aktionen durchführen:

Geräte mit Chrome-Browser und ChromeOS, die Zugriff auf Ihre Unternehmensdaten haben, in Bestandslisten aufnehmen. Die Endpunktprüfung für den Gerätebestand stellt Ihnen wichtige Informationen bereit, mit denen Sie kontinuierlich für die benötigte Sicherheit sorgen können. In Kombination mit dem kontextsensitiven Zugriff unterstützt die Endpunktprüfung Sie beim Erzwingen einer detaillierten Zugriffssteuerung.

Durch Warnmeldungen vor Phishingangriffen in Echtzeit Unternehmensdaten besser schützen. Dank dem Echtzeit-Scannen von URLs mithilfe der intelligenten Google-Funktion Safe Browsing stellen Sie sicher, dass Ihre Nutzer nicht aus Versehen schädliche Websites aufrufen (Abbildung 2).

Verdächtige Dateien in Echtzeit stoppen, bevor sie Sicherheitslücken in Ihrem Netzwerk ausnutzen. Chrome stellt Dateiscans und -analysen in Echtzeit direkt in Google Cloud bereit (Abbildung 3).

Sie können einstellen, ob Nutzer bereits vor der Analyse auf die entsprechende Datei zugreifen dürfen oder warten müssen, bis sie vollständig geprüft wurde. Außerdem unterstützt Chrome eine dreistufige Malware-Erkennung auf Grundlage einer Reputationsprüfung, einer statischen Analyse und erweiterter Cloud-Sandbox-Funktionen.

Sowohl versehentliche als auch absichtliche Exfiltrationen von Unternehmensdaten verhindern. Datenlecks lassen sich vermeiden. Mit vorkonfigurierten und benutzerdefinierten Regeln können Sie Aktionen blockieren oder Nutzer benachrichtigen lassen, wenn Uploads auf Websites gegen die Unternehmensrichtlinien verstoßen. Dies eignet sich insbesondere für Unternehmen, die mit Kundendaten interagieren, deren Schutz gesetzlichen Compliancevorgaben unterliegt (Abbildung 4).

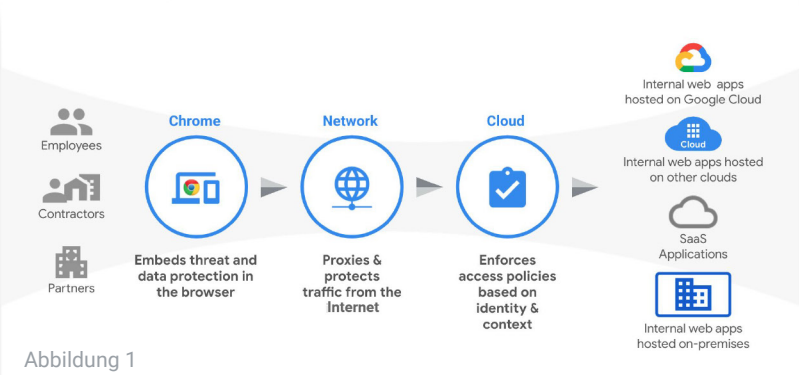


Abbildung 1

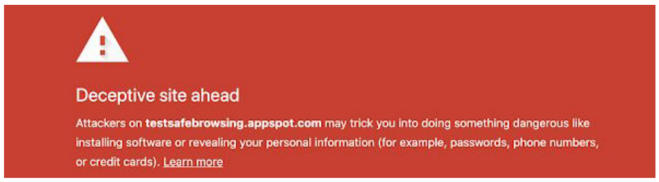


Abbildung 3

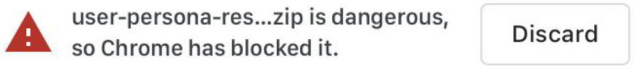


Abbildung 3

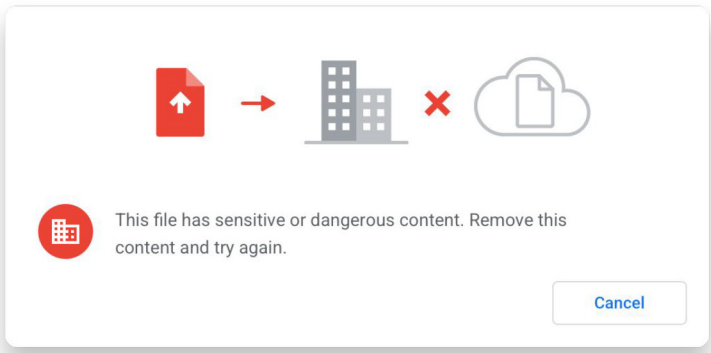
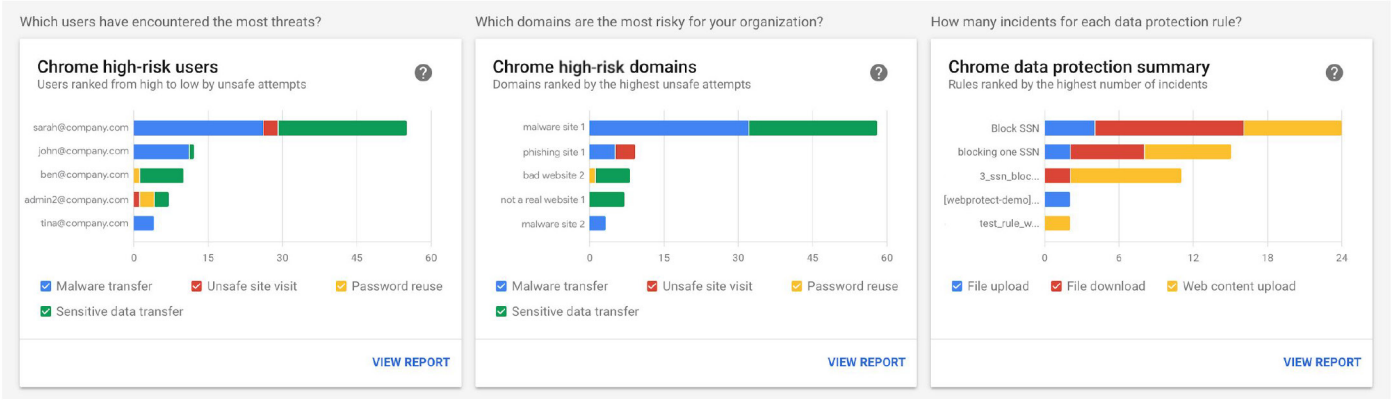


Abbildung 4

chrome enterprise

Benachrichtigungen, Protokolle und Berichte zu verdächtigen Aktivitäten. IT-Teams können die Sicherheits- und Compliancevorgaben ihrer Organisation dank zusätzlicher Einblicke in Sicherheitsereignisse rund um verdächtige Downloads, URLs, die Wiederverwendung von Passwörtern und potenzielle Datenlecks besser umsetzen. Außerdem lassen sich auf Grundlage dieser Informationen riskante Verhaltensweisen und Nutzer mit hohem Risiko identifizieren.



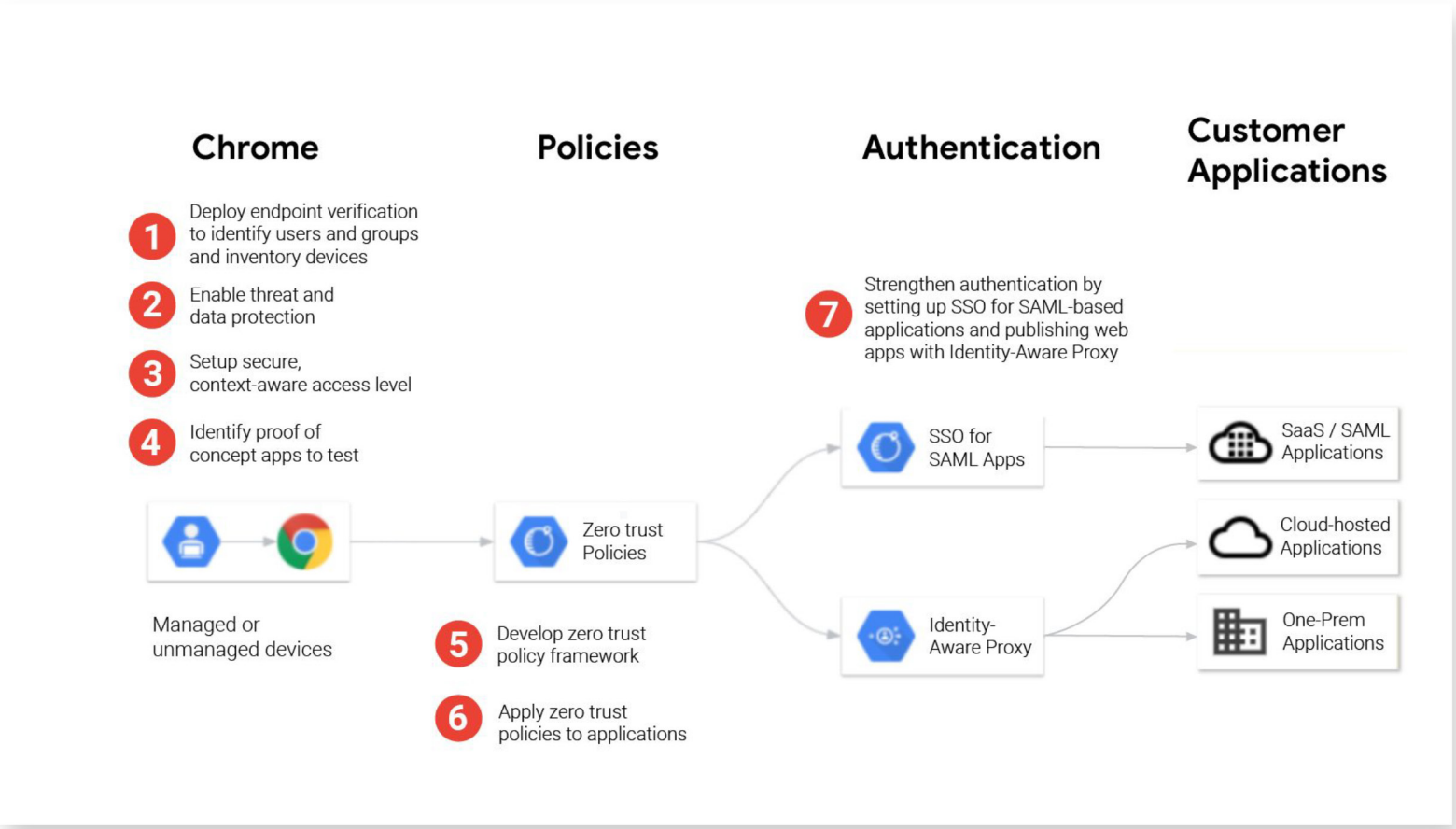
Verbesserte Zero-Trust-Sicherheit – dank ChromeOS

Zusätzlich zu den Vorteilen des erweiterten Schutzes vor Bedrohungen und den Datenschutzfunktionen in Chrome können Sie mit ChromeOS für noch mehr Sicherheit sorgen. Als von Grund auf sicheres Betriebssystem handelt es sich bei ChromeOS um einen wichtigen Enabler für Zero-Trust-Sicherheitsmodelle.

In Kombination mit dem Chrome-Browser und BeyondCorp Enterprise kann ChromeOS dafür sorgen, dass Risiken in Unternehmen sowohl auf der Hardware-Ebene als auch in internen und externen Anwendungen sowie bis ins offene Web hinaus gemindert werden.

Zu BeyondCorp Enterprise migrieren

Jeden Netzwerknutzer und jede Anwendung zum Zero-Trust-Framework von BeyondCorp Enterprise zu migrieren, dauert seine Zeit. Mit der phasenweisen Migration reduzieren Sie das Risiko von Betriebsunterbrechungen und können größere Gruppen von Netzwerknutzern auf BeyondCorp Enterprise verschieben, ohne dabei ihre Produktivität zu beeinflussen.



Fazit

Mit Chrome Enterprise und BeyondCorp Enterprise können Unternehmen ihr Zero-Trust-Sicherheitsframework leichter umsetzen. Traditionelle, perimeterbasierte Sicherheitsmodelle sind heutzutage nicht länger effektiv – insbesondere durch das vermehrte mobile Arbeiten. Organisationen mit mobilen Mitarbeitern an verschiedenen Standorten oder im Homeoffice müssen den Zugriff auf wichtige geschäftliche Anwendungen und Dienste daher auf einfache und sichere Weise ermöglichen.

Mit BeyondCorp Enterprise erhalten Unternehmen wichtige Einblicke in unsichere Aktivitäten und profitieren von Chrome-Funktionen für Datenschutz und den Schutz vor Bedrohungen, darunter zusätzliche Sicherheitsebenen gegen Phishingangriffe, Malware und Datenverlust.

Weitere Informationen zu BeyondCorp Enterprise finden Sie unter q.co/cloud/bce.

chrome enterprise

Ressourcen

Um Ihr Wissen über den Chrome-Browser, ChromeOS, Chrome Enterprise und BeyondCorp Enterprise zu vertiefen, empfehlen wir Ihnen außerdem das folgende Infomaterial:

Chrome-Browser

- Chrome-Browser für Ihr Unternehmen herunterladen
- Weitere Informationen zum Support für Google Chrome für Unternehmen
- Versionshinweise für Chrome Enterprise und Education
- Mit dem Chrome Releases-Blog immer über die neuesten Aktualisierungen auf dem Laufenden bleiben
- Offizieller Google-Blog zu Sicherheit und Schutz
- Die Chrome Enterprise und Education-Hilfe und das Google Chrome-Hilfeforum
- Weitere Möglichkeiten mit der Chrome-Verwaltung über die Cloud
- Google Chrome-Datenschutzhinweise
- Google Chrome-Whitepaper zum Thema Datenschutz

ChromeOS

- Weitere Informationen zum Cloud-First-Betriebssystem von Google
- Chromium-Blog

Chrome Enterprise

- Weitere Informationen darüber, wie Sie mit Google Chrome Enterprise die Unternehmensfunktionen von ChromeOS, Chrome-Browser und Chrome-Geräten optimal nutzen können
- Chrome Enterprise-Blog

BeyondCorp Enterprise

- Weitere Informationen zu BeyondCorp Enterprise
- BeyondCorp Enterprise-Blog

BeyondCorp Enterprise